CHAPTER 2

POLICY

A. PHYSICAL SECURITY PROGRAM

1. The physical security program is defined as that part of security concerned with active and passive measures designed - to prevent unauthorized access to personnel, equipment, installations, materiel and documents, and to safeguard them against espionage, sabotage, damage, and theft. Physical security is a primary command responsibility.

2. Physical security programs provide the means to counter threats during peacetime, transition to war, and in wartime. Physical security threats include the following:

a. Foreign intelligence services.

b. Paramilitary forces.

c. Terrorists and saboteurs.

d. Criminals.

e. Protest groups.

f. Disaffected persons.

3. Physical security planning includes the following:

a. Using electronic security systems to reduce both vulnerability to the threat and reliance on fixed security forces.

b. Integration of physical security into contingency, mobilization, and wartime plans, and testing of physical security procedures and measures during the exercise of these plans.

c. Coordinating with installation operations security, crime prevention, information security, personnel security, communications security, automated information security and physical security programs to provide an integrated and coherent effort.

d. Training security forces at facilities or sites in tactical defense against, and response to, attempted penetrations.

e. Creating and sustaining physical security awareness.

f. Identifying resource requirements to apply adequate measures.

4. Physical security measures are a combination of active or passive systems, devices, and security personnel used to protect a security interest from possible threats. These measures include:

a. Security forces and owner or user personnel.

b. Military working dogs.

c. Physical barriers, facility hardening and active delay or denial systems.

d. Secure locking systems, containers, and vaults.

e. Intrusion detection systems.

f. Assessment or surveillance systems (i.e., closed-circuit television or thermal imagers).

g. Protective lighting.

h. Badging systems, access control devices, materiel or asset tagging systems, and contraband detection equipment.

B. RESPONSIBILITIES

The DoD Component shall designate a point of contact to oversee the physical security program. The oversight function includes the following:

1. Develop necessary standard policies and procedures to supplement the provisions of this regulation to meet specific needs, including joint supplementation, when possible.

2. Coordinate and maintain liaison with the other Departments and Agencies on physical security matters.

3. Establish procedures for sharing threat information expeditiously through law enforcement and intelligence channels.

4. Formalize security procedures for joint response to terrorist incidents.

5. Develop specific physical security threat assessments and update them annually or as needed.

6. Coordinate the acquisition of physical security equipment and establish procedures to identify requirements for related research as described in DoD Directive 3224.3 (reference (j)).

7. Develop training, qualification, and suitability requirements for dedicated security forces (including contract

security forces where not prohibited), security technicians and physical security specialists.

C. SECURITY SYSTEM PERFORMANCE GOAL

1. The goal of the security system for an asset or facility is to deploy security resources so as to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage or other criminal activity. To achieve this goal a security system provides the capability to detect, assess, communicate, delay and respond to an unauthorized attempt at entry.

2. The components of a security system each have a function and related measures which provide an integrated capability for the following:

a. Detection, accomplished through human, animal or electronic means, alerts security personnel to possible threats and attempts at unauthorized entry at or shortly after time of occurrence;

b. Assessment, through use of video subsystems, patrols or fixed posts, assists in localizing and determining the size and intention of an unauthorized intrusion or activity;

c. Command and control, through diverse and secure communications to ensure that all countermeasures contribute to preventing or containing sabotage, theft or other criminal activity;

d. Delay, through the use of active and passive security measures, including barriers, impedes intruders in their efforts to reach their objective;

e. Response, through the use of designated, trained and properly equipped security forces. Detection, and delay must provide sufficient warning and protection to the asset until the response force can be expected to arrive at the scene.

D. PHYSICAL SECURITY THREAT MATRIX

At Figure 2-1 is a description of the DoD generic threat types developed for the physical security program. Using these threat types as a guide, commanders shall develop program, system, command or installation threat statements which assess potential security threats *to* critical assets. Using both law enforcement and intelligence information, these assessments should categorize opportunity (when possible) and capabilities of potential adversaries. Physical security threat statements will be used for the development of security systems tailored to the protection of assets and items of security interest.

THREATTYPE	THREAT DESCRIPTION	THREAT EXAMPLE
MAXIMUM	**INDIVIDUALS IN ORGANIZED** AND TRAINED GROUPS ALONE OR WITH ASSISTANCE FROM AN INSIDER; SKILLED ARMED AND EQUIPPED INTRUDERS WITH PENETRATION AIDS	TERRORISTS AND SPECIAL PURPOSE FORCES; HIGHLY TRAINED INTELLIGENCE AGENTS
ADVANCED	INDIVIDUAL(S) WORKING ALONE OR IN COLLUSION WITH AN INSIDER; SKILLED OR SEMISKILLED WITHOUT PENETRATION AIDS	HIGHLY ORGANIZED CRIMINAL ELEMENTS; TERRORISTS OR PARAMILITARY FORCES; FOREIGN INTELLIGENCE AGENTS WITH ACCESS
INTERMEDIATE	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE OR IN SMALL GROUPS; SOME KNOWLEDGE OR FAMILIARITY OF SECURITY SYSTEM	CAREER CRIMINALS; ORGANIZED CRIME; WHITE COLLAR CRIMINALS; ACTIVE DEMONSTRATORS; COVERT INTELLIGENCE COLLECTORS; SOME TERRORIST GROUPS
LOW	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE OR IN A SMALL GROUP	CASUAL INTRUDERS; PILFERERS AND THIEVES; OVERT INTELLIGENCE COLLECTORS; PASSIVE DEMONSTRATORS

Figure 2-1. Physical Security Threat Matrix

E. PRIORITIZATION OF ASSETS

At Figure 2-2 is a description of the DoD resource and asset prioritization scheme with examples of typical assets, a criticality definition, and an example of a typical security system for each level. DoD Components shall develop appropriate operational concepts or security standards to meet the performance goal of paragraph C against the type of threats defined in paragraph D for critical assets designated by the Component under each security system level. Security system levels are assigned to critical assets or major systems in security planning documents to ensure that minimum security standards are met. Commanders are responsible for higher levels of security afforded personnel, equipment and assets within the command depending on regional threat.

F. PHYSICAL SECURITY PLANNING AND SYSTEM ACQUISITION

DoD Components shall establish procedures to ensure that physical security planning for the acquisition of major systems is appropriate, and in accordance with paragraph E above. One management solution is provided by MIL-STD-1785 (reference (l)).

G. PROTECTIVE DESIGN AND MILITARY CONSTRUCTION

DoD Components shall establish procedures to ensure that all military construction projects are reviewed at the conceptual stage and throughout the process so that appropriate physical security, antiterrorist or protective design features are incorporated into the design. Use MIL-HNBK-1013/l (reference (k)) or other approved security engineering guidance for information.

H. SECURITY OF LEASED FACILITIES

DoD Components shall establish procedures to ensure that leases for DoD activities resident within commercial facilities include provisions for positive physical security of DoD occupied areas.

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
A INTEGRATED ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, ACCESS DELAY AND DENIAL SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED IMMEDIATE RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE WILL RESULT IN GREAT HARM TO THE STRATEGIC CAPABILITY OF THE UNITED STATES	NUCLEAR AND CHEMICAL WEAPONS AND ALERT/MATED DELIVERY SYSTEMS CRITICAL COMMAND, CONTROL AND COMMUNICATIONS FACILITIES AND SYSTEMS CRITICAL INTELLIGENCE GATHERING FACILITIES AND SYSTEMS PRESIDENTIAL TRANSPORT SYSTEMS NUCLEAR REACTORS AND CATEGORY I AND II SPECIAL NUCLEAR MATERIALS RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
B ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EXPECTED TO GRAVELY HARM THE OPERATIONAL CAPABILITY OF THE UNITED STATES	ALERT SYSTEMS, FORCES, AND FACILITIES ESSENTIAL COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY I ARMS, AMMUNITION, AND EXPLOSIVES RESEARCH, DEVELOPMENT AND TEST ASSETS

Figure 2-2. **Resource and Asset Priorities**

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
C ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIERS, SECURITY PATROLS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD IMPACT UPON THE TACTICAL CAPABILITY OF THE UNITED STATES	NONALERT RESOURCES AND ASSETS PRECISION GUIDED MUNITIONS COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY II ARMS, AMMUNITION AND EXPLOSIVES POL/POWER/ WATER ISUPPLY STORAGE FACILITIES RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
D ELECTRONIC SECURITY SYSTEMS, **ACCESS CONTROLS, BARRIERS, DESIGNATED RESPONSE** FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD **COMPROMISE THE DEFENSE INFRASTRUCTURE OF** THE UNITED STATES	ARMS, AMMUNITION, AND EXPLOSIVES EXCHANGES AND COMMISSARIES, FUND ACTIVITIES CONTROLLED DRUGS AND PRECIOUS METALS TRAINING ASSETS RESEARCH, DEVELOPMENT AND TEST ASSETS